UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,871	01/30/2004	Hiroshi Kobata	11365-052001	4081

26171 7590 06/07/2007

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DADA, BEEMNET W	
ART UNIT	**PAPER NUMBER**
2135	
MAIL DATE	**DELIVERY MODE**
06/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/766,871	KOBATA ET AL.	
	Examiner	Art Unit	
	Beemnet W. Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11 have been examined.

Claim Objections

2. The numbering of claims is not in accordance with 37 CFR 1.126 which requires the original numbering of the claims to be preserved throughout the prosecution. When new claims are presented, they must be numbered consecutively beginning with the number next following the highest numbered claims previously presented (whether entered or not).

Misnumbered claims A1, B1, B2, C1 and C2 have been renumbered 1, 8, 9, 10 and 11 respectively.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3 and 8-11 are rejected under 35 U.S.C. 102(e) as being anticipated by Okereke et al. US 2003/0196084 A1 (based on effective filing date of provisional application 60/371,736) [hereinafter referred to as Okereke].

5. As per claim 1, Okereke teaches a system for authenticating a user, the system comprising:

a sending system connected to a network and comprising a processor connected to a storage device (page 2, paragraph 0024 and figure 4), one or more input/output devices (i.e., user interface, keyboard etc., paragraphs 0024 & 0026), and a port for communicating through the network (i.e., local area connection, paragraph 0024) wherein the processor is configured to send a digital certificate (i.e., forwarding PKI certificate, paragraph 0026), a password associated with a user identity (i.e., credential information, paragraph 0026), and a hardware identifier (i.e., unique identifier, paragraph 0025) that is associated with the sending system over the network to a server system and to execute software using a secure layer protocol located between an application layer and a transport layer (i.e., secure IP network session, paragraphs 0025 & 0026], and

the server system (i.e., proxy server) connected to the network to receive the digital certificate (i.e., receiving PKI certificate, paragraph 0026), a password associated with a user identity (i.e., credential information, paragraph 0026), and a hardware identifier (i.e., unique identifier, paragraph 0025), the server system comprising a processor configured to execute software located between the application layer and the transport layer capable of authenticating (i.e., secure IP network session, paragraphs 0025 and 0026), based on the received digital certificate and the received password, a user identity of the sending system and authenticating, based on the received the hardware identifier, the sending system [paragraphs 0025-0026].

6. As per claim 8, Okereke teaches an authentication proxy server connected to a network, the authentication proxy server comprising a processor connected to a storage device, one or more input/output devices, and a port for communicating through the network wherein the processor is configured to receive a digital certificate (i.e., proxy server receiving PKI certificate, paragraph 0026), a password associated with a user identity (i.e., credential information,

paragraph 0026), and a hardware identifier (i.e., unique identifier, paragraph 0025), and execute software logically operating between an application layer and a transport layer of a communications protocol stack for the purpose of authenticating, based on the received digital certificate and the received password, a user identity of a client system associated with the digital certificate and password, and authenticating, based on the received the hardware identifier, the client system (i.e., authenticating the user device and creating secure IP network session, paragraphs 0025 and 0026).

7. As per claim 2, Okereke further teaches the system wherein the processor of the sending system is further configured to send a public key over the network to the server system, and the processor of the server system is further configured to receive the public key and the executing software is further capable of authenticating the user identify of the sending system based on both the received digital certificate and the received public key (i.e., PKI certificate, paragraphs 0026).

8. As per claim 3, Okereke further teaches the system wherein the server system is further configured to: determine permitted access to content associated with the server system, and allow only permitted access to the content associated with the server system [paragraphs 0036 and 0026].

9. As per claim 9, Okereke further teaches the system wherein digital certificate includes an identification of the certificate authority that issued the digital certificate and a public key of a sending system associated with the digital certificate such that the public key has been encrypted with the private key of the certificate authority, and the processor is further configured

to execute software logically operating between the application layer and the transport layer: receive a public key of a sending system associated with the digital certificate, use the public key of the certificate authority to decrypt the public key of the sending system included in the digital certificate, and authenticate the user identity when the decrypted public key corresponds to the received public key (i.e., PKI authentication scheme, paragraphs 0026-0027].

10. As per claims 10 and 11, Okereke further teaches the system wherein client software application provides a specialized communication protocol for communicating with the authentication proxy server client software application provides a specialized authentication protocol for authenticating with the authentication proxy server client software application provides a specialized security protocol for encrypting and decrypting communication data with the authentication proxy server and the client software application contains an hypertext markup rendering module that will display decrypted data from the authentication proxy in a secure fashion, preventing user access to the data in any manner other than through the rendered display (i.e., installed client application, paragraph 0025).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Okereke et al. US 2003/0196084 A1 in view of Primak et al. US 6,389,448 B1 (hereinafter Primak).

13. As per claim 4, Okereke teaches a sending system connected to a network and a server system (i.e., proxy server) connected to the network [paragraphs 0024-0026]. Okereke is silent on the server system comprising multiple servers and one or more of processors of the server system are further configured to perform load balancing of network connection requests across the multiple servers. However, load balancing of network connection is old and well known in the art, which has the advantage of enhancing speed and efficiency of a system. For example, Primak teaches a server system comprising multiple servers and one or more of processors of the server system are further configured to perform load balancing of network connection requests across the multiple servers [column 2, lines 32-44]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Primak within the system of Okereke in order to enhance efficiency of the system.

14. Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okereke et al. US 2003/0196084 A1 in view of Harrison US 2002/0166064 A1.

15. As per claims 5-7, Okereke teaches a sending system connected to a network and comprising a processor connected to a storage device (page 2, paragraph 0024 and figure 4), one or more input/output devices (i.e., user interface, keyboard etc., paragraphs 0024 & 0026), and a port for communicating through the network (i.e., local area connection, paragraph 0024) wherein the processor is configured to send a digital certificate (i.e., forwarding PKI certificate, paragraph 0026), a password associated with a user identity (i.e., credential information,

paragraph 0026), and a hardware identifier (i.e., unique identifier, paragraph 0025). Okereke is silent on creating a digital signature associated with a hardware component of the sending system, and encrypt the hardware identifier. However, generating a digital signature and encrypting the hardware identifier is well known in the art. For example, within the same field of endeavor, Harrison teaches a data authentication system, including creating a digital signature associated with a hardware component of a sending system, encrypting a hardware identifier and sending the encrypted hardware identifier [see Harrison, paragraphs 0008, 0009 and 0013]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Harrison within the system of okereke in order to enhance the security of the system.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Beemnet W Dada

May 22, 2007

KIM VU
SUPERVISORY PATENT
TECHNOLOGY C